Mais de 143.000 arquivos de malware segmentam usuários do Android e iO

Data: 2025-09-05 23:30:59

Autor: Inteligência Against Invaders

No segundo trimestre de 2025, os usuários dos dispositivos Android e iOS enfrentaram ameaças

cibernéticas implacáveis, com a Kaspersky Security Network relatando quase 143.000 pacotes de

instalação maliciosos detectados em seus produtos de segurança móvel.

Embora o número geral de ataques móveis – incluindo malware, adware e software potencialmente indesejado – tenha sido de 10,71 milhões no segundo trimestre, os Trojans permaneceram o perigo predominante, representando 31,69 % de todas as ameaças detectadas.

Entre abril e junho de 2025, a Kaspersky Solutions bloqueou 10,71 milhões de ataques móveis. Isso representou um declínio do Q1, amplamente impulsionado por uma redução significativa nas campanhas relacionadas ao RiskTool.androidos.spyloan-aplicativos empréstimos incorporados a estruturas que colhem dados de mutuários, como listas de contatos, às vezes encontradas pré-instalações em dispositivos.

Nesse período, Kaspersky identificou 142.762 pacotes de instalação para malware Android e aplicativos indesejados, incluindo:

- 42.220 Trojans bancários móveis
- 695 Ransomware Mobile Trojans

Trojans bancários mantiveram a parte superior entre os tipos de malware, com a família Mamont dominando. Os Trojans Spy caíram para o quinto lugar quando a onda de SMS roubando Trojan-spy.androidos.Agent.akg diminuiu, e agente.amw spyware disfarçado de aplicativos de cassino também diminuíram. Os aplicativos e adware indesejados do tipo RiskTool seguiram a prevalência, enquanto os Trojans da Família Triada compreendiam a maior parte da categoria genérica de Trojan.

Várias ameaças novas e incomuns surgiram no segundo trimestre:

Um ladrão de plataforma cruzada apelidada endereçado Os usuários do Android e do iOS, exfiltrando imagens de galerias de dispositivos.

A análise vinculou esta campanha ao malware sparkcat anterior descoberto em lojas de aplicativos, com páginas de aplicativos maliciosos imitando instalações legítimas.

Sparkkitty Acredita -se que o objetivo principal seja o roubo de códigos de recuperação da carteira de criptomoeda salvos como capturas de tela.

Em uma nova reviravolta, os atacantes incorporaram um SDK com capacidade de DDoS nos aplicativos de visualizador de conteúdo para adultos. Uma vez instalado, esses aplicativos

transformam dispositivos móveis que consentiram em bots capazes de enviar inundações de tráfego configuráveis ??para endereços projetados por atacantes-a criatividade dos cibercriminosos da cibercriminal ao explorar usuários inocentes

Posando como um cliente VPN que aprimora a privacidade, este Trojan aproveita o serviço de ouvinte de notificação do Android para interceptar senhas únicas (OTPs) de aplicativos de mensagens e redes sociais.

Em vez de fornecer cobertura de VPN, ela retransmite silenciosamente os códigos interceptados para os atacantes via Bots Telegram, facilitando a aquisição de contas.

Hotspots geográficos

As tendências de malware específicas da região destacaram surtos locais:

- Em Türkiye, Coper Banking Trojans (Variantes .C e .A) atingiram mais de 97 % dos usuários direcionados por essas famílias.
- A Índia viu os droppers e os trojans bancários da Recompensa afetando 95 % de sua base de usuários vitimizados.
- O Uzbequistão enfrentou FakeApp.hy e Piom.bkzj Trojans, massando como aplicativos de busca de emprego e utilidade, coletando dados pessoais de 85 a 87 % de seus usuários atacados.
- O Brasil encontrou o Pylcasa Droppers disfarçado de ferramentas simples, como calculadoras, que então redirecionaram as vítimas para as páginas da web de cassino ilícitas ou ilícitas.

Trojans bancários móveis, embora ligeiramente mais baixos no Q2 do que o Q1, permaneceram assustadoramente prevalecentes. Kaspersky Detectaram 42.220 pacotes de Trojan bancários, com variantes de Mamont compreendendo 57,7 % desse total.

Entre as 10 principais famílias de Trojan bancárias, o Mamont.DA aumentou de 26,68 % para 30,28 % dos usuários atacados, enquanto o recém -chegado Mamont.ev saltou para 17 %.

Apesar de um declínio modesto em ataques móveis gerais durante o segundo trimestre de 2025, o cenário de ameaças móveis continua a evoluir com campanhas sofisticadas de Trojan, surtos regionais e ladrões de plataforma cruzada.

Trojans bancários, liderados pela prolífica família de Mamont, juntamente com os novos Trojans com capacidades de DDoS e OTP, destacam os riscos persistentes que os usuários móveis enfrentam. A vigilância, atualizações regulares de software e soluções robustas de segurança móvel continuam sendo defesas essenciais contra esses adversários sempre adaptáveis.

Encontre esta história interessante! Siga -nosLinkedIneXPara obter mais atualizações instantâneas.